REMARKS/ARGUMENTS

Claims 1-67 are pending in the present application. Claims 1, 4, 5, 7, 12, 13, 20, 22, 24-26, 29, 30, 32, 37, 38, 45, 47, 50, 51, 53, 58, 59 and 66 have been amended herewith. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 1-4, 6-7, 9-10, 13-20, 22-29, 31-32, 34-35, 38-45, 47-50, 52-53, 55-56 and 59-66 under 35 U.S.C. § 102(b) as being anticipated by Dotan (5,822,517 A). This rejection is respectfully traversed.

Per the features of the pending claims, an improved data protection system is provided wherein data is journaled to provide an improved ability to dynamically recover data using the journaled data.

Specifically with respect to Claim 1, such claim has been amended in accordance with Applicants' Specification at page 3, lines 8-11, page 5, line 22 – page 6, line 21, et seq., to clearly differentiate the claimed journaling process from the teachings of the cited reference where an initial state of a program to be executed is compared to a final state of this same program file after execution (Dotan Abstract). The problem with Dotan's technique is that the virus is only detected *after* the program has completed execution, whereas per the present invention, such virus detection is *dynamically determined during program execution* to thereby advantageously provide a timelier virus detection system where viruses can be detected early on to mitigate damage.

Further, the features of Claim 1 advantageously provide an ability to *protect/restore data associated with an executing program*. For example, a payroll program executing on a data processing system may maintain employee data records in an employee database, such as in external storage 112 or 114 of Figure 1. Per the features provided by Claim 1, such employee data records can be restored if adversely impacted by a virus due to the data journaling capability provided by the features of Claim 1. Per the teachings of the cited Dotan reference, only the actual executable program itself can be restored (col. 4, lines 20-27 and lines 45-64).

It is thus urged that this amendment to Claim 1 has overcome the present 35 USC 102(b) rejection.

Applicants initially traverse the rejection of Claims 2-4, 6-7 and 9-10 for reasons given above with respect to Claim 1 (of which Claims 2-4, 6-7 and 9-10 depend upon).

Further with respect to Claim 4, such claim has been amended to specify details with respect to the pattern matching, and it is urged that the cited reference does not teach such pattern matching and therefore it is further urged that Claim 4 is not anticipated by the cited reference.

With respect to Claim 13, such claim has been amended to clearly differentiate the claimed *data object* access from the teachings of the cited reference, where an initial state of a *program to be executed* is compared to a final state of this same executable program after execution (Dotan Abstract). The problem with Dotan's technique is that the virus is only detected after the program has completed execution, whereas per the present invention, such virus detection is dynamically determined during program execution to thereby advantageously provide a timelier virus detection system where viruses can be detected early on to mitigate damage. Another disadvantage of Dotan's technique is that is only protects against damage to the actual executable program itself, and provides no protection for data associated with such executable program, such as data maintained in a separate file or database that is accessed by an executable program. It is thus urged that this amendment to Claim 13 has overcome the present 35 USC 102(b) rejection.

Applicants initially traverse the rejection of Claims 14-20 for reasons given above with respect to Claim 13 (of which Claims 14-20 depend upon).

Further with respect to Claim 14, it is urged that the cited reference does not teach the claimed 'repeating' step, where *in response to a determination that an unauthorized intrusion is absent*, another pattern compare operation is performed. Claim 14 expressly recites "*responsive to an absence of the unauthorized intrusion*, repeating the comparing step using another pattern from the set of patterns" (emphasis added). The only thing described in the cited reference that occurs *in response to a determination that an unauthorized intrusion is absent* is an end of program (FIG 4, blocks 60 and 62). Thus, as every element of the claimed invention is not identically shown in a single reference, it is further urged that Claim 14 has been erroneously rejected under 35 USC 102(b).

Further with respect to Claim 15, it is urged that the cited reference does not teach the claimed 'time threshold' determination that is done if it is determined that an unauthorized intrusion is absent. Claim 15 expressly recites "*if an intrusion is absent*, determining whether a time threshold has been reached" (emphasis added). The only thing described in the cited reference that occurs *in response to a determination that an unauthorized intrusion is absent* is an end of program (FIG 4, blocks 60 and 62). Thus, as every element of the claimed invention is not identically shown in a single reference, it is further urged that Claim 15 has been erroneously rejected under 35 USC 102(b)[1].

Still further with respect to Claim 15, the Examiner equates Dotan's alarm signal (FIG 4, block 64) as being the same as the claimed threshold. Applicants urge that Claim 15 expressly recites a 'time

[1] For a prior art reference to anticipate in terms of 35 U.S.C. 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990) (emphasis added).

threshold', and a determination being made with respect to such time threshold ("determining whether a time threshold has been reached"), which is very different from generation of an alarm signal as per the teachings of the cited reference. Thus, as every element of the claimed invention is not identically shown in a single reference, it is further urged that Claim 15 has been erroneously rejected under 35 USC 102(b).

Further with respect to Claim 17, it is urged that the cited reference does not teach the claimed feature of "wherein match between the pattern and the set of actions identifies a presence of the unauthorized intrusion". The Examiner states that the cited reference teaches this at FIG 4, blocks 60 and 64. Applicants respectfully submit that to the contrary, blocks 60 and 64 deal with the situation of no match (see the word 'NO' coming out of block 60 and leading to block 64). A 'no match' does not teach a 'match'. Thus, as every element of the claimed invention is not identically shown in a single reference, it is further urged that Claim 17 has been erroneously rejected under 35 USC 102 (b).

Still further with respect to Claim 17, it is urged that the Examiner them self stated, in rejected Claim 16, that a match indicates absence of an unauthorized intrusion. It is logically inconsistent to state that a match indicates *absence* of an unauthorized intrusion (in rejecting Claim 16), and then stating (in rejecting Claim 17) that a match indicates *presence* of an unauthorized intrusion. If a match indicates both an absence and a presence of an unauthorized intrusion, there would be no way to determine whether an unauthorized intrusion occurred, which is the primary functionality provided by the cited reference. Such an interpretation (a match indicates both an unauthorized intrusion as well as an authorized intrusion) results in a failure of the cited reference to achieve its expressed, intended purpose – evidencing an unreasonable and illogical interpretation of such reference teachings. Thus, it is further urged that Claim 17 has been erroneously rejected under 35 USC 102(b) as every element of the claimed invention is not identically shown in a single reference.

With respect to Claim 20, such claim has been amended to clearly distinguish the claimed data objects – whose states are saved – from the actual executable program as described by the cited reference. As amended, Claim 20 defines the data objects to be objects that are dynamically accessed by executing processes within the data processing system. In contrast, the cited reference merely saves the actual executable program itself prior to its execution, for compare with the actual executable program itself after its execution. The features of Claim 20 advantageously provide an ability to *protect/restore data associated with an executing program*. Per the teachings of the cited Dotan reference, only the actual executable program itself can be restored (col. 4, lines 20-27 and lines 45-64). Thus, it is further urged that Claim 20 is not anticipated by the cited reference.

With respect to Claim 22 (and similarly for Claim 23), such claim is directed to an intrusion detection system that comprises both (1) a sensor filter that receives requests from a process to access data within the data processing system, and (2) a journaler that journals data in response to accessing of

the data (such data being the same data that the process is requesting access to, such requests to access such data being received by the sensor filter). This can be seen in the preferred embodiment at FIG 3 of Applicants' Specification, where sensor filter 300 receives data access requests from process 218, and journaler 304 that journals such data requested by process 218. In rejecting Claim 22, the Examiner states that the claimed sensor filter is taught by the cited reference at FIG 4, block 52; col. 6, lines 14-18 and col. 4, lines 27-30. Applicants urge that block 52 of FIG 4 merely states "Program has been invoked", and a mere invocation of a program does not teach any type of a sensor filter that receives requests from a process to access data within the data processing system. As to the passage cited at col. 6, such passage merely describes that a CPU loads an executable program into memory, begins processing such program, and while being processed, such program may invoke a second executable program. Such program execution and invocation of a second executable program does not teach any type of a sensor filter that receives requests from a process to access data within the data processing system. Rather, this passage describes a CPU, a first executable program and a second executable program. There is no description of any type of component, such as the claimed sensor filter, that *receives requests from a process to access data*. As to the passage cited at col. 4, lines 27-30, such passage merely describes 'that the invented method' is invoked prior to the loading of a program stored in memory. Invoking a method prior to program execution does not teach any type of a sensor filter that receives requests from a process to access data within the data processing system. Thus, for this reason alone (no teaching in the cited reference of the claimed sensor filter), it is urged that Claim 22 (and similarly for Claim 23) has been erroneously rejected as every element of the claimed invention is not identically shown in a single reference.

Additionally, and as described above, Claim 22 also recites a journaler that journals data in response to accessing of the data (such data being the same data that the process is requesting access to, such requests to access such data being received by the sensor filter). In rejecting this aspect of Claim 22, the Examiner cites step 68 and associated text; and col. 7, lines 37-51. As there is no step 68 in the cited reference, there is no associated text for such non-existent step, and thus this non-existent step 68 and associated text does not teach the claimed journaler, as they don't exist. As to the cited passage at col. 7, such passage describes *restoring* a program. A process step of restoring data does not in any way teach a journaler that *journals data in response to accessing of the data* (such data being the same data that the process is requesting access to, such requests to access such data being received by the sensor filter). It is therefore further urged that Claim 22 (and similarly for Claim 23) has been erroneously rejected under 35 USC 102(b), as every element of the claimed invention is not identically shown in a single reference – and in particular (i) the sensor filter and (ii) the jounaler and (iii) the synergistic co-action between the sensor filter, jounaler and pattern matcher.

Applicants traverse the rejection of Claims 24 for similar reasons to those given above with respect to Claim 1.

Applicants traverse the rejection of Claim 25 for similar reasons to those given above with respect to Claim 13.

Applicants traverse the rejection of Claims 26-29, 31-32 and 34-35 for similar reasons to those given above with respect to Claims 1-4, 6-7 and 9-10.

Applicants traverse the rejection of Claims 38-45 for similar reasons to those given above with respect to Claims 13-20.

Applicants traverse the rejection of Claims 47-50, 52-53 and 55-56 for similar reasons to those given above with respect to Claims 1-4, 6-7 and 9-10.

Applicants traverse the rejection of Claims 59-66 for similar reasons to those given above with respect to Claims 13-20.

Therefore, the rejection of Claims 1-4, 6-7, 9-10, 13-20, 22-29, 31-32, 34-35, 38-45, 47-50, 52-53, 55-56 and 59-66 under 35 U.S.C. § 102 has been overcome.

II. 35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 5, 8, 11, 12, 21, 30, 33, 36, 37, 46, 51, 54, 57, 58 and 67 under 35 U.S.C. § 103 as being unpatentable over Dotan (5,822,517 A) in view of Conklin et al (5,991,881 A).

This rejection is initially traversed for reasons given above with respect to the missing claimed features identified above with respect to independent Claims 1, 13, 24-26, 38, 47 and 59, and urge that the additional cited Conkin reference does not overcome such teaching deficiencies identified above.

Further with respect to Claim 5 (and similarly for Claims 30 and 51), such claim has been amended to clarify that the journaling of data is with respect to data that is located in a storage device external to the data processing system. This claimed feature advantageously allows for using the journaled intrusion detection system in environments where a data processing system may access data that is external to such data processing system (Specification page 6, line 22 – page 7, line 1, et seq.). In rejecting Claim 5, the Examiner states that this claimed feature is taught by the cited Conklin reference at Conklin's Figures 3 and 4 and associated text where the storage within the hosts is external to the monitoring system. Applicants urge that such teaching is not directed to data *that is journaled*, as required by Claim 5 in combination with Claim 1, and therefore it is urged that Claim 5 is not obvious in view of the cited references as there are claimed features not taught or suggested by any of the cited references.

Further with respect to Claim 8 (and similarly for Claims 33 and 54), such claim recites "responsive to an identification of the virus, blocking access to the data by a process accessing the data".

In rejecting Claim 8, the Examiner cites Conklin's teaching at col. 5, lines 34-38 as teaching this claimed feature. While this passage describes an action that is responsive to an identification of a reportable activity, the action that is described is different from the action that is claimed in Claim 8. Specifically, Claim 8 recites that *access to the data is blocked*. In contrast, the action described by Conklin at col. 5 is that a data packet is written to a log file. No type of *blocking action* is described at all. Rather, a log writing action is described in this cited passage. This can also be seen by the fact that if there is no indication of a reportable activity such as an intrusion, the packet is discarded (col. 5, lines 23-26). Quite simply, this passage describes either the discarding (if no intrusion) or logging (if an intrusion) of a packet. There is no description of any type of blocking access to the data in response to an identification of a virus. Therefore, a prima facie case of obviousness has not been established with respect to Claim 8[2], and accordingly the burden has not shifted to Applicants to rebut the (improper) obviousness assertion[3]. In addition, as a prima facie case of obviousness has not been established, Claim 8 has been erroneously rejected[4].

Further with respect to Claim 11 (and similarly for Claims 36 and 57), such claim recites that "the journaled data is stored in a protected memory accessible only by the method". In rejecting Claim 11, the Examiner cites Conklin's Figure 9 and associated text as teaching that the journaled data is stored in a protected memory accessible only by the method. Applicants urge that Conklin's Figure 9 does not describe any type of protected memory, as claimed, but instead describes an alert notification process (col. 2, lines 38-39; col. 8, lines 20-24). No type of memory, either a protected memory (as claimed) or otherwise is shown in Conklin's Figure 9.

Still further with respect to Claim 11, Conklin does not describe any type of journaled data (as defined per Claim 1), and thus it necessarily follows that since there is no teaching of journaled data, there is no teaching of storing such non-existent journaled data, either into a protected memory as claimed or anywhere else.

Therefore, a prima facie case of obviousness has not been established with respect to Claim 11, and accordingly the burden has not shifted to Applicants to rebut the (improper) obviousness assertion. In

---

[2] To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974) (emphasis added by Applicants).

[3] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. *Id.*

[4] If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

addition, as a prima facie case of obviousness has not been established, Claim 11 has been erroneously rejected.

Further with respect to Claim 12 (and similarly for Claims 37 and 58), such claim recites that "the journaled data is stored in a data structure located in a protected memory inaccessible by a process". In rejecting Claim 12, the Examiner cites Conklin's Figure 5 and associated text as teaching this claimed feature. Applicants urge that such figure describes a data packet, and not journaled data (as defined per Claim 1). In addition, this Figure 5 and associated text does not describe that any type of data structure is *inaccessible* by a process, as required by Claim 12. Therefore, a prima facie case of obviousness has not been established with respect to Claim 12, and accordingly the burden has not shifted to Applicants to rebut the (improper) obviousness assertion. In addition, as a prima facie case of obviousness has not been established, Claim 12 has been erroneously rejected.

Further with respect to Claim 21 (and similarly for Claims 46 and 67), Applicants traverse the rejection of such claim for similar reasons to the further reasons given above with respect to Claim 5.

Therefore, the rejection of Claims 5, 8, 11, 12, 21, 30, 33, 36, 37, 46, 51, 54, 57, 58 and 67 under 35 U.S.C. § 103 has been overcome.

III. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: June 26, 2006

Respectfully submitted,

Brian D. Owens
Reg. No. 55,517
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants